

BILLS AS WELL AS VALUABLE PAPERS MOUNTING IC CHIP AND PREVENTING METHOD OF UNFAIR UTILIZATION OF THEM

Publication number: JP2001260580

Publication date: 2001-09-25

Inventor: TODA YUKITOSHI

Applicant: HITACHI LTD

Classification:

- International: **B42D15/10; G06K17/00; G06K19/00; G06K19/07; G06Q10/00; G06Q40/00; G07D7/02; B42D15/10; G06K17/00; G06K19/00; G06K19/07; G06Q10/00; G06Q40/00; G07D7/00; (IPC1-7): B42D15/10; G06F17/60; G06K17/00; G06K19/00; G06K19/07; G07D7/02**

- european:

Application number: JP20000077750 20000315

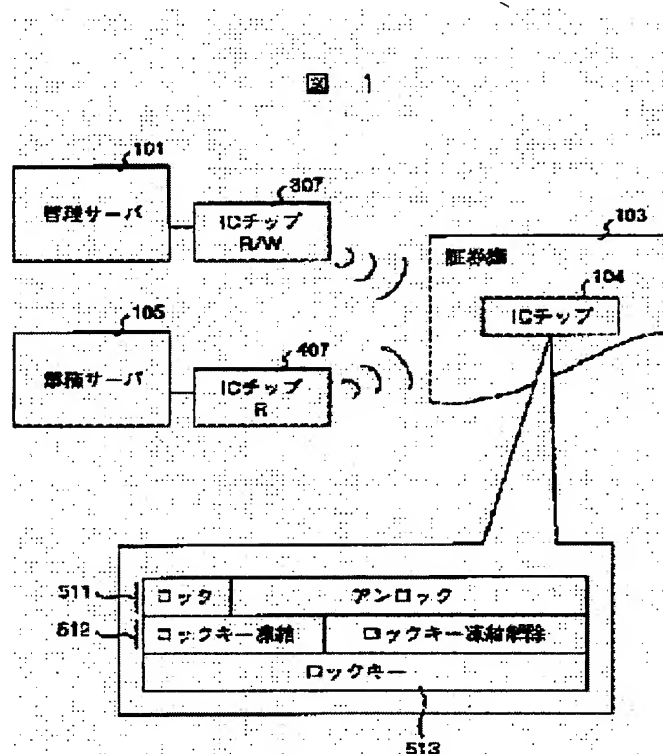
Priority number(s): JP20000077750 20000315

Report a data error here

Abstract of JP2001260580

PROBLEM TO BE SOLVED: To provide valuable papers, capable of preventing unfair utilization by discriminating the cheating of the same and capable of reutilizing the papers when the papers can be taken back to a regular control source, and the preventing method of unfair utilization of them.

SOLUTION: A fine IC chip 104 is mounted on valuable papers 103, such as bills, stocks or the like, while the memory device of the IC chip 104 stores a lock information 511 and a lock key. The lock information 511 retains a condition of either one of lock/unlock. A business server 105 reads the condition of the lock information 511 through an IC chip reading device 407 and will not start a business process when the condition is not under the condition of unlock. A control server 101 communicates with the IC chip 104 through an IC chip reading and writing device 307 to certify that the lock key 513 is right and, thereafter, changes the condition of the lock information 511 if necessary.



Data supplied from the esp@cenet database - Worldwide

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-260580

(P2001-260580A)

(43) 公開日 平成13年9月25日 (2001.9.25)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
B 4 2 D 15/10	5 3 1	B 4 2 D 15/10	5 3 1 B 2 C 0 0 5
	5 2 1		5 2 1 3 E 0 4 1
G 0 6 F 17/60	2 1 4	G 0 6 F 17/60	2 1 4 5 B 0 3 5
	5 1 0		5 1 0 5 B 0 4 9
	5 1 2		5 1 2 5 B 0 5 5

審査請求 未請求 請求項の数 5 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願2000-77750 (P2000-77750)

(22) 出願日 平成12年3月15日 (2000.3.15)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 戸田 幸利

神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所サービス事業部内

(74) 代理人 100068504

弁理士 小川 勝男 (外1名)

最終頁に続く

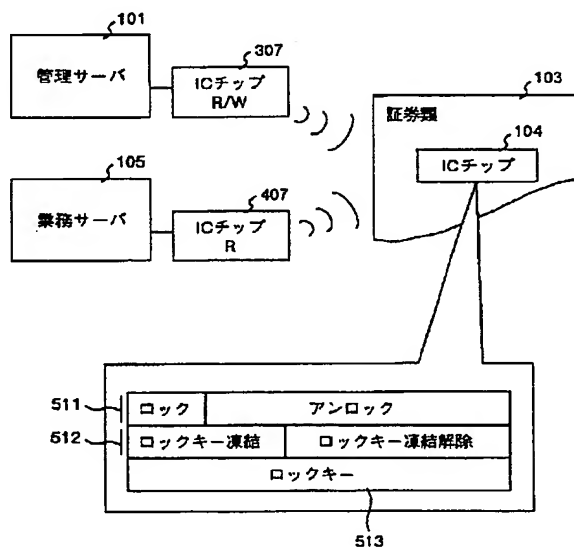
(54) 【発明の名称】 ICチップを搭載する紙幣及び有価証券類並びにその不正利用防止方法

(57) 【要約】

【課題】 証券類が搾取されたことを識別して不正利用を防ぐとともに、正規な管理元に取り戻せた場合には再利用が可能な証券類及びその不正利用防止方法を提供する。

【解決手段】 紙幣、株券など有価証券類103に微細なICチップ104が搭載されており、ICチップ104の記憶装置はロック情報511及びロックキーを格納する。ロック情報511はロック／アンロックいずれかの状態を保持する。業務サーバ105は、ICチップ読取装置407を介してロック情報511の状態を読み取り、それがアンロック状態でなければ業務処理を開始しない。管理サーバ101は、ICチップ読取・書込装置307を介してICチップ104と通信し、ロックキー513が正しいものと認証した後に、必要に応じてロック情報511の状態を変更する。

図 1



【特許請求の範囲】

【請求項 1】非接触で読み書き可能な IC チップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記 IC チップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能な情報と、外部からの要求に応答して前記情報を変更する前記 IC チップ内で実行可能なプログラムとを格納する記憶装置を有することを特徴とする IC チップを搭載する有価証券類。

【請求項 2】非接触で読み書き可能な IC チップを搭載する紙幣、商品券、株券、債券など有価の証券類の不正利用防止方法であって、前記 IC チップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック／アンロック情報と、外部からの要求に応答して前記ロック／アンロック情報の参照と更新を行う前記 IC チップ内で実行可能なプログラムとを格納する記憶装置を有し、前記証券類の利用を禁止するように外部の計算機によって前記 IC チップに前記ロック／アンロック情報をロック状態に設定するように指令し、前記証券類を利用可能とするように外部の計算機によって前記 IC チップに前記ロック／アンロック情報をアンロック状態に設定するように指令し、外部の計算機によって前記 IC チップ上の前記ロック／アンロック情報を参照し、前記ロック／アンロック情報がアンロック状態の場合に業務処理を開始することを特徴とする IC チップを搭載する有価証券類の不正利用防止方法。

【請求項 3】前記ロック／アンロック情報を更新する前記外部の計算機は、その記憶装置に第 1 のキー情報を保存し、前記 IC チップはその記憶装置に第 1 のキー情報と対になる第 2 のキー情報を保存し、前記ロック／アンロック情報を更新する前記外部の計算機と前記 IC チップとの間で第 1 のキー情報と第 2 のキー情報とが所定の対応関係をもつことを認証したとき、前記 IC チップによって前記ロック／アンロック情報の更新を行うことを特徴とする請求項 2 記載の IC チップを搭載する有価証券類の不正利用防止方法。

【請求項 4】非接触で読み書き可能な IC チップを搭載する紙幣、商品券、株券、債券など有価の証券類であって、前記 IC チップは、前記証券類を業務処理に利用可能か否かを示す書き換え可能なロック／アンロック情報と、外部からの要求に応答して前記ロック／アンロック情報の参照と更新を行う前記 IC チップ内で実行可能なプログラムとを格納する記憶装置を有するところの有価証券類と、前記 IC チップに対して前記ロック／アンロック情報を更新するよう指令する管理用計算機と、前記 IC チップに要求して前記ロック／アンロック情報を参照し、前記ロック／アンロック情報がアンロック状態の場合に業務処理を開始する業務処理用計算機とを有することを特徴とする IC チップを搭載する有価証券類の不正利用防止システム。

【請求項 5】前記ロック／アンロック情報を更新する前

記管理用計算機は、その記憶装置に第 1 のキー情報を保存し、前記 IC チップはその記憶装置に第 1 のキー情報と対になる第 2 のキー情報を保存し、前記ロック／アンロック情報を更新する前記管理用計算機と前記 IC チップとの間で第 1 のキー情報と第 2 のキー情報とが所定の対応関係をもつことを認証したとき、前記 IC チップが前記ロック／アンロック情報の更新を行うことを特徴とする請求項 4 記載の IC チップを搭載する有価証券類の不正利用防止システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、金融／サービス／運送業などの取扱い対象となる証券類及びその不正利用防止方法に係わり、特に紙幣、商品券、株券、債券、手形、小切手など何らかの価値を持つ有価証券類（以下、単に証券類と呼ぶ）を保管、運搬する際に盗難等で不正に取得した証券類を使用不可の状態にしたり、正規に入手した証券類の有効性を証明する不正利用防止システムに適用して有効な技術に関するものである。

20 【0002】

【従来の技術】従来、取引の支払いをしたり、商品の引換えをしたり、株式会社に投資したり、第三者から事業資金を得たり、代金の支払いの約束をしたり、金銭の支払いの約束をしたりと、様々な価値をもつ権利を表す証券類が世の中に流通している。

【0003】これらの証券類を一時的に保管したり、運搬したりする場合には、物理的な鍵のかかる金庫やトランクなどに鍵を掛けたり、盗難を防ぐために警備員を配置したりするが、証券類には特に何らかの加工を加えることはせず、現状はそのまま利用可能な状態にある。

30 【0004】なお、近年は街頭に置かれた無人の ATM / CD 端末を、パワーシャベルなどといった重機を使って破壊し、保管してある現金を搾取したりすることがあるので、ATM / CD 端末に破壊などの不正行為を働いた場合に、紙幣にインクを吹き付けたりして盗難にあった事実を記したりする技術がある。

【0005】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。すなわち一旦盗難にあった証券類は、正規に利用されるものと区別のつかない状態にあって不正に利用されたり、インクなどの目印が付いてしまい、正当な所有者が取り戻すことができて再活用できないという問題がある。またインクが搾取される証券類の全数に確実につかない可能性もある。

【0006】本発明の目的は上記問題を解決し、盗難された証券類の不正利用を防止したり、正規の管理元に取戻した場合に再利用することが可能な証券類及びその不正利用防止方法を提供することにある。

【0007】

50 【課題を解決するための手段】本発明は、保管または輸

送される証券類について、証券類に搭載したICチップの情報を読んで、不正に搾取されたものとして利用してはならないか、あるいは正規に譲渡されたものとして利用して良いものかどうかを識別可能にするものである。

【0008】本発明において、証券類の利用の可否を識別するには、証券類に搭載したICチップに利用可否の識別情報を登録することによって行う。近年になってサイズが数ミリ(2~3mm)角の非接触通信式のICチップ(RFID)の開発が新聞等で発表されてきている。こういった微細なICチップ製造技術がさらに進めば、紙幣や有価証券などに装着できるようなICチップが登場する。本発明では、こういった紙などの薄い媒体に微細なICチップを本発明でいう証券類の一枚ずつに搭載し、当該証券類各々の有効性の情報をもたせ、それらの情報を読み込んで識別することを可能にするものである。

【0009】証券類に搭載するICチップへの読み書きは、当該証券類を保管/運搬の管理をする法人または事業所の管理単位に可能であり、ICチップへの情報の書き込みに関するセキュリティも管理する。よって正規の管理元が保管または運搬する証券類を他者が搾取したとき、当該証券類に搭載するICチップの情報が利用不可の状態であることを示すようにしておき、証券類の利用時にこの情報を読み出すことによって、当該証券類が不正に搾取されたものであることを識別でき、これらをこの状態で利用することを拒否することによって、不正利用を防止することが可能になる。証券類に搭載するICチップの情報の読み取りは、証券類を業務処理に使用する際にICチップ読取装置で読み取ることができるようしておく。

【0010】一方、証券類に搭載したICチップへの情報の書き込みは、セキュリティのための制御情報(暗証番号、暗号鍵など)により、このような制御情報を保持する管理用計算機のみが行えるようにし、制御情報を知らない第三者がICチップの情報を書き換えることはできないようにする。

【0011】またある管理元が管理する証券類を別の管理元に正規に移管する場合には、新しい管理元が譲渡対象となる証券類に搭載するICチップの情報を書き換えるために必要な独自の制御情報に変更できるように、古い管理元が設定していた制御情報を用いて制御情報の書き換え制限を解除することにより、新しい管理元が管理する制御情報に変更することができる。こうして新たな管理元は、自分の管理下のセキュリティ制御情報を用いて証券類に搭載するICチップの情報を必要に応じて書き換えることができるようになる。

【0012】よって一旦不正に搾取された証券類でも、元のICチップの情報を書き換えできる正当なセキュリティ制御情報をもつ管理元に戻せば、利用不可状態となっていた証券類のICチップの情報を利用可能な状態

に戻すことができ、問題なく再利用することができるようになる。

【0013】以上のように本発明の証券類及びその不正利用防止方法によれば、非接触の通信によりICチップを搭載した管理単位全数について確実に証券類の利用可否の情報を読み書きできるので、搾取された証券類を識別でき、その不正利用を防ぐことができ、さらに正規の所有者の手に戻れば再度利用可能な状態に戻すことも可能である。

【0014】

【発明の実施の形態】以下に証券類の不正利用防止を可能とする実施形態について図面を用いて説明する。

【0015】図1は、本実施形態の概略構成を示す図である。証券類103には微細なICチップ104が装着されている。ICチップ104は、証券類103を構成する2枚の紙の間にすき込むか、あるいはICチップ104を封入したシールを証券類103に接着するなどの方法によって証券類103に装着されている。いずれにしてもICチップ104は、証券類103を使用不可能にするほど破損することなく、そのICチップ104を証券類103から引き離すことができないような方法で証券類103に装着されている。ICチップ104内の記憶装置にはロック情報511、ロックキー凍結情報512及びロックキー513を記録する。ロック情報511は、ロック状態とアンロック状態のいずれかの状態をもつ。ロック状態は業務処理のために証券類103を利用できない状態であり、アンロック状態は業務処理のために証券類103を利用できる状態である。ロックキー513は、ロック情報511、ロックキー凍結情報512およびロックキー513自体を変更するために必要な鍵(パスワード、暗号鍵など)となるビット列である。ロックキー凍結情報512は、ロックキー凍結状態とロックキー凍結解除状態のいずれかの状態をもつ。ロックキー凍結状態はロックキー513を凍結し更新できない状態であり、ロックキー凍結解除状態はロックキー513を更新できる状態である。

【0016】管理サーバ101は、ロック情報511、ロックキー凍結情報512及びロックキー513を更新する権限をもち、ロックキー513を管理する計算機であり、ICチップ読取・書込装置307を接続する。管理サーバ101は、ICチップ読取・書込装置307を介して証券類103に搭載されたICチップ104上の情報を非接触で読み取り、ロック情報511の変更、ロックキー凍結情報512の変更及びロックキー513の更新を行う。

【0017】業務サーバ105は、証券類103に関する業務処理を行う計算機であり、ICチップ読取装置407を接続する。業務サーバ105は、ICチップ読取装置407を介して証券類103のICチップ104上のロック情報511にアクセスし、ロック情報511が

アンロック状態であれば証券類103を取り扱う業務処理を行い、ロック状態であれば業務処理を行わない。

【0018】図2は、ICチップ104の装着された証券類103を利用する手順の例を説明する図である。ICチップ104の装着された証券類103は、証券類103の製造過程から入ってきた証券類103であり最初に利用されるものであるか、または他の管理サーバによって管理されていたものであって最初に当該管理サーバ101の管理下に入るものとし、ロック情報511がロ

ック状態、ロックキー凍結情報512がロックキー凍結の状態にあるものとする。

【0019】図2(a)は、管理サーバ101が証券類103上のICチップ104についてロックキー凍結情報512をロックキー凍結解除し、ロックキー513を自分の管理するロックキーに更新するステップである。図2(b)は、管理サーバ101が証券類103上のICチップ104についてロック情報511をロック状態にし、ロックキー凍結情報512をロックキー凍結の状態に変更するステップである。図2(c)は、この状態の証券類103を保管または運搬するステップを示す。この状態の証券類103を業務処理に利用することはできない。また他の管理サーバによって不当にロックキー513を自分の管理下のロックキーに更新することはできない。

【0020】図2(d)は、この証券類103を業務処理に利用するために、管理サーバ101が証券類103上のICチップ104についてロック情報511をアンロックの状態に変更するステップである。図2(e)では、業務サーバ105が証券類103上のICチップ104のロック情報511にアクセスして利用の可否をチェ

ックする。ロック情報511がアンロック状態であればこの証券類103に関する業務処理を開始し、ロック情報511がロック状態であればこの証券類103についての業務処理を行わない。従って保管または運搬中に盗難等に会った証券類103は業務処理されない。

【0021】上記の証券類103がある管理サーバの管理下から別の管理サーバの管理下に移るとは、例えば証券類103がある金融機関から別の金融機関に譲渡されたり、事業所間で譲渡される場合を想定している。従ってセキュリティの問題が生じないのであれば、ICチップ104のロック情報511がアンロック、ロックキー凍結情報512がロックキー凍結解除の状態で証券類103を事業所間で譲渡しても構わない。

【0022】図3は、管理サーバ101の概略構成を示す図である。図3に示すように管理サーバ101は、CPU301と、メモリ302と、磁気ディスク装置303と、キーボード装置304と、ディスプレイ装置305と、CD-ROM装置306と、ICチップ読取・書込装置307を有している。磁気ディスク装置303はロックキー管理テーブル308を格納している。管理サ

サーバ101の全体が携帯情報処理装置であってもよい。

【0023】CPU301は、管理サーバ101全体の動作を制御する装置である。メモリ302は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置303は、各種処理プログラムやデータを格納しておく記憶装置である。キーボード装置304は、データ入力のための装置であり、ディスプレイ装置305は各種データの表示を行う装置である。CD-ROM装置306は、各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。ICチップ読取・書込装置307は、証券類103に搭載するICチップ104との間で非接触で情報の読み書きをする装置である。

【0024】ロックキー管理テーブル308は、当該管理サーバ101が管理するロックキーを格納するテーブルである。

【0025】ロック/ロックキー処理部310は、メモリ302に格納され、図2に示すように証券類103のICチップ104に記録されたロック情報511、ロックキー凍結情報512及びロックキー513の管理に係わる処理を行うプログラムであり、CPU301によって実行される。

【0026】CD-ROM等の記録媒体に記録されたロック/ロックキー処理部310を磁気ディスク装置303等に格納した後、メモリ302にロードして実行するものとする。なおこのプログラムを記録する記録媒体としてCD-ROM以外の他の記録媒体でも良い。

【0027】図4は、業務サーバ105の概略構成を示す図である。図4に示すように業務サーバ105は、CPU401と、メモリ402と、磁気ディスク装置403と、キーボード装置404と、ディスプレイ装置405と、CD-ROM装置406と、ICチップ読取装置407とを有している。

【0028】CPU401は、業務サーバ105全体の動作を制御する装置である。メモリ402は、各種処理プログラムやデータを格納する記憶装置である。磁気ディスク装置403は、各種処理プログラムやデータを格納しておく記憶装置である。ICチップ読取装置407は、証券類103に搭載するICチップ104から非接触でロック情報511を読み取る装置である。

【0029】メモリ402は、ロック判定処理部410及び業務処理部411を格納する。ロック判定処理部410は、証券類103に搭載するICチップ104のロック情報511を読み込み、当該証券類103の利用の可否を判定する処理を行うプログラムである。業務処理部411は、利用可能と判定した証券類103に関する業務アプリケーションの処理を行う処理部である。

【0030】CD-ROM等の記録媒体に記録されたロック判定処理部410を含むプログラムを磁気ディスク装置403等に格納した後、メモリにロードして実行す

るものとする。なおこのプログラムを記録する記録媒体としてCD-ROM以外の他の記録媒体でも良い。

【0031】図5は、証券類103に搭載されるICチップ104の内部構成を示す図である。ICチップ104は、微細な半導体チップであり、図5に示すように通信アンテナ501、電磁誘導起電装置502、電力蓄積装置503、制御装置504及び記憶装置505を有している。

【0032】通信アンテナ501は、ICチップ104とICチップ読取・書込装置307又はICチップ読取装置407との間で情報を送受信したり、ICチップ104を駆動する電源となる電力供給のための電磁波をICチップ読取・書込装置307又はICチップ読取装置407から受けたりする装置である。電磁誘導起電装置502は、通信アンテナ501で受けた電磁波を電磁誘導により電力に変換する装置である。電力蓄積装置503は、電磁誘導起電装置502で起電した電力を蓄積して、ICチップ104を駆動するための電源とする装置である。

【0033】制御装置504は、マイクロプロセッサを含み、ICチップ104全体の動作を制御する装置である。記憶装置505は、ロック情報511、ロックキー凍結情報512及びロックキー513の管理情報と、暗号復号プログラム521、ロックキー正否判定プログラム522、ロック状態参照更新プログラム523、ロックキー更新プログラム524など各種プログラムを格納する。

【0034】ロック情報511は、ロック／アンロックの状態を示す1ビットの情報を格納する。ロックキー凍結情報512は、ロックキー凍結／ロックキー凍結解除を示す1ビットの情報を格納する。ロックキー513は当該ICチップ104に付与される鍵として管理される情報である。

【0035】図6は、ICチップ104に記録されるロック情報511及びロックキー凍結情報512の状態遷移について説明する図である。ロック情報511及びロックキー凍結情報512の状態は、ロックかつロックキー凍結の状態601と、アンロックかつロックキー凍結の状態602と、アンロックかつロックキー凍結解除の状態603の3つがある。

【0036】状態601は、当該証券類103を利用不可能で、かつロックキー513を更新することができない状態である。正しいロックキーを用いることによって状態601から状態602に遷移することができる。

【0037】状態602は、当該証券類103を利用することが可能で、かつロックキー513を更新することができない状態である。正しいロックキーを用いることによって状態602から状態603に遷移することができる。また正しいロックキーを用いることによって状態602から状態601に遷移することができる。

【0038】状態603は、当該証券類103を利用することが可能で、かつロックキー513を更新することができる状態である。正しいロックキーを用いることによって状態603から状態602に遷移することができる。

【0039】図7A及び図7Bは、管理サーバ101のロック／ロックキー処理部310の処理の流れを示すフローチャートである。ロック／ロックキー処理部310は、対象とする証券類103についてキーボード等から入力された要求を受け取る（ステップ701）。要求は次に示す4種類ある。(1)当該証券類103に搭載されたICチップ104のロック情報511をアンロック状態からロック状態に変更する。(2)ロック情報511をロック状態からアンロック状態に変更する。この要求ではロックキー凍結情報512をロックキー凍結状態にするか、ロックキー凍結解除の状態にするかの指定が必要である。(3)ロック情報511をアンロック状態、ロックキー凍結情報512をロックキー凍結解除状態にした後にロックキー513を更新する。(4)ロックキー513を更新した後にロック情報511をロック状態、ロックキー凍結情報512をロックキー凍結状態にする。

【0040】次にロック／ロックキー処理部310は、ロックキー513が正しいか否か、例えば古い管理元から通知を受けたロックキーであってキーボード304などから入力されたロックキー又はロックキー管理テーブル308に登録されているロックキーとICチップ104上のロックキー513とが一致するか否かを判定する（ステップ702）。ここではまだロックキー513が更新されていないため、ロックキー更新前のロックキーについて照合することになり、そのロックキーは当該管理サーバ101が管理するロックキー又は他の管理事業所から通知を受けたロックキーのいずれかである。ロックキー513が正しくなければ（ステップ702、誤り）、処理終了とする。

【0041】ロックキー513が正しいければ、当該ICチップ104上のロック情報511をアンロック状態に変更するアンロック処理を行う（ステップ703）。次にロックキーの更新が要求されていないければ（ステップ704、しない）、ステップ709へ行く。ロックキーの更新が要求されている場合には、ロックキー513が正しいか否かを判定する（ステップ705）。ここではステップ702のチェックが繰り返されることになり、ロックキー513が正しいと判定される。次にロックキー凍結情報512を読み取り、ロックキー凍結状態であれば（ステップ706、凍結）、これをロックキー凍結解除の状態にする（ステップ707）。次にロックキー管理テーブル308を参照してICチップ104上のロックキー513を管理サーバ101の管理下にある新しいロックキーに更新する（ステップ708）。

【0042】次に図7Bに移り、ロック／ロックキー処理部310は、ロックキーを凍結するか否か判定する（ステップ709）。要求（1）、（4）及び（2）でロックキー凍結の指定がされた場合にはロックキーの凍結が必要である。ロックキー凍結しない場合にはステップ712へ行く。次にロックキー513が正しいか否か判定する（ステップ710）。ステップ708のロックキー更新をした場合には、ロックキー管理テーブル308上のロックキーと更新後のロックキー513との一致が判定されるわけであり、当然ロックキー513が正しいと判定される。ステップ708のロックキー更新をしていない場合には、ステップ702のチェックが繰り返されることになり、ロックキー513が正しいと判定される。ロックキーが正しいければ（ステップ710、正しい）、ロックキー凍結情報512をロックキー凍結状態にする（ステップ711）。

【0043】次にロック／ロックキー処理部310は、ロック情報511をロック状態にするか否か判定する（ステップ712）。要求（1）および（4）については、ロック情報511をロック状態にする必要がある。ロックする場合（ステップ712、する）には、再びロックキー513が正しいか否か判定する（ステップ713）。要求（1）及び（4）の場合にはステップ702及びステップ710のチェックが繰り返されることになり、ロックキー513が正しいと判定される。ロックキーが正しいければ（ステップ713、正しい）、ロックキー凍結情報512が凍結の状態であり（ステップ714、凍結）、ロック情報511がアンロック状態の場合に（ステップ715、アンロック）、ロック情報511をロック状態に変更するロック処理を行う（ステップ716）。

【0044】ステップ710でロックキーの誤りがある場合、ステップ712でロックしない場合、ステップ713でロックキーの誤りがある場合、ステップ714でステップ709の判定と矛盾するロックキー凍結情報512がロックキー凍結解除状態の場合、およびステップ715でロック情報511がロック状態の場合には直ちに処理終了とする。

【0045】上記実施形態では、ロックキー513が正しいか否かのチェックは、別の管理下にあったロックキー又はロックキー管理テーブル308上のロックキーとICチップ104上のロックキー513とが一致するか否かの判定によっていたが、管理サーバ101からICチップ読取・書込装置307を介してICチップ104へ平文のままのロックキーを伝送したり、ICチップ104から管理サーバ101へ平文のままのロックキーを伝送すると、セキュリティが破られる危険性が高くなる。たとえばICチップ読取・書込装置307から送出される電磁波を盗聴すれば管理サーバ101とICチップ104との間に伝送されるロックキーを知り得ること

になる。このような危険を避けるために、直接ロックキーを伝送せずにロックキーを暗号鍵とし、ロックキーによって暗号化した数値を伝送するのが望ましい。たとえばロックキー管理テーブル308に登録するロックキーを公開鍵とし、ロック／ロックキー処理部310が乱数を発生させ、発生した乱数をこの公開鍵で暗号化して暗号化した乱数と元の乱数とをICチップ104へ伝送する。ICチップ104のロックキー正否判定プログラム522は、ロックキー正否判定のコマンドを受けたとき、暗号復号プログラム521が秘密鍵として保存するロックキー513によって暗号化された乱数を復号し、ロックキー正否判定プログラム522が復号された乱数と元の乱数とを比較してロックキーの正否を判定し、その結果（正または否）を管理サーバ101のロック／ロックキー処理部310に通知することが可能である。この場合には別の管理下にあったロックキー又はロックキー管理テーブル308上のロックキーとICチップ104上のロックキー513とは公開鍵ペアの対応関係を持ち、一般に同一値とはならない。従って一般にはいずれかの管理下にあるロックキーとICチップ104上のロックキー513とは同一値である必要はなく、所定の対応関係をもった数値であればよい。

【0046】ICチップ104上のロック状態参照更新プログラム523は、管理サーバ101又は業務サーバ105からそのロック情報511の参照を要求するコマンドを受けたとき、ロックキーの正否が判定済であるなしに係わらずロック情報511の内容を要求元に送信する。しかしロック情報511の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。またロック状態参照更新プログラム523は、ロックキー凍結情報512の参照又は更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。

【0047】同様にICチップ104上のロックキー更新プログラム524は、ロックキー513の更新を要求するコマンドを受けたとき、ロックキー正否判定プログラム522によってロックキーが正しいとの判定をした後でなければ、この要求に応答しない。ロックキーとして公開鍵ペアを使用する場合には、ロック／ロックキー処理部310は、ICチップ104へロックキー513の更新要求コマンドを伝送して応答を得た後に、更新後のロックキー（秘密鍵）を古いロックキー（公開鍵）で暗号化してICチップ104へ送信する。ロックキー更新プログラム524は、暗号復号プログラム521を介して受け取った暗号化情報をロックキー513に格納される古いロックキー（秘密鍵）で復号し、ロックキー513を復号された新しいロックキー（秘密鍵）に置き換える。ロックキーとして公開鍵ペアの代わりに共通鍵を

使用する場合には、同様にロック／ロックキー処理部310が新しいロックキー（共通鍵）を古いロックキー（共通鍵）で暗号化してICチップ104へ送信し、ロックキー更新プログラム524が受け取った暗号化情報を古いロックキー（共通鍵）で復号し、ロックキー513を得られたロックキーに置き換える。

【0048】ロックキー正否判定プログラム522は、記憶装置505上にロックキー正否判定フラグをもち、ロックキーの正否判定の結果（正または否）を保存する。そしてステップ703の処理（アンロック処理）、ステップ708の処理（ロックキーの更新）、ステップ711の処理（ロックキーの凍結処理）及びステップ716の処理（ロック処理）の各々の処理終了時にこのロックキー正否判定フラグを初期状態（否）にリセットする。このような構成によって要求（1）～（4）のいずれの場合にも処理終了時にこのフラグが否の状態にリセットされている。

【0049】なお上記実施形態ではICチップ104にロックキー凍結情報512を設け、ロックキー凍結情報512がロックキー凍結解除状態のときのみロックキー513を更新可能としたが、ロックキー凍結情報512を設けず、ロック情報511の状態に係わらずロックキーが正しい場合には常にロックキー513更新可能とするように縮退した形でも本発明を実施できる。その場合には要求は（1）及び（2）と（3）又は（4）の3種類となり、ステップ706、707、709、710、711及び714の処理は除外される。

【0050】またICチップ104の記憶装置505に当該ICチップ104の製造番号のような識別番号（ID）をもたせ、ロックキー管理テーブル308にはこのIDとロックキーとの対応テーブルを設け、IDとロックキーとの対応ICチップ104を搭載した証券類103を管理してもよい。またICチップ104を単に保管又は輸送中の盗難防止という目的で使用するのであれば、管理サーバ101が管理下におくすべての証券類103のICチップ104に同一のロックキーを付与して管理することも可能である。盗難等から取り戻されたロック状態におかれたICチップ104を搭載する証券類103は、当該管理サーバ101のみがアンロックの状態にできる。

【0051】あるいは上記実施形態についての変形例として、ICチップ104のロック情報511に対し、あらかじめ特別に規定したロックキー513の無効を示す値を設定すると、永久にアンロック状態に戻れない仕組みにしておけば、例えば使用後の商品券を再使用できないように裁断（廃棄）処理するなどと同様に、本発明の証券類に対して、電子的な廃棄処理を施すことができる。

【0052】以上述べたように、本発明の実施に当って

は色々の変形ができるので、セキュリティの必要程度とICチップ104のコストとの兼ね合いで、ICチップ104のハードウェア及びICチップ104に格納しICチップ104が実行するプログラムの機能を決めればよい。

【0053】上記のように本実施形態では、当該証券類に対する業務処理の実行の可否を業務サーバが管理サーバにオンラインネットワークなどで問い合わせることなく、当該証券類に搭載したICチップの情報から判定し、正当に業務処理を行ったり、不正な利用を防止したりすることが可能である。また本発明の方法を適用し、一旦搾取された利用不可能な証券類を正当な管理サーバの管理下に取り戻せた場合は、その再利用を可能とすることができる。

【0054】以上説明したように本実施形態によれば、証券類に搭載したICチップの情報を用いて当該証券類の利用の可否を判定できるので、不正に搾取された証券類かどうかをその場で識別して不正利用を未然に防ぐことが可能である。

【0055】

【発明の効果】本発明によれば、証券類に搭載したICチップの情報を用いて不正に搾取された証券類を識別できるので、不正利用を防止することができ正当な管理元に戻せた場合に再利用可能な状態に戻すことが可能である。

【図面の簡単な説明】

【図1】実施形態の概略構成を示す図である。

【図2】実施形態のICチップを搭載する証券類の利用手順を説明する図である。

【図3】実施形態の管理サーバ101の概略構成を示す図である。

【図4】実施形態の業務サーバ105の概略構成を示す図である。

【図5】実施形態の証券類103に搭載されるICチップ104の内部構成を示す図である。

【図6】実施形態のロック情報511及びロックキー凍結情報512の状態遷移を示す図である。

【図7A】実施形態の管理サーバ101のロック／ロックキー処理部310の処理手順を示すフローチャートである。

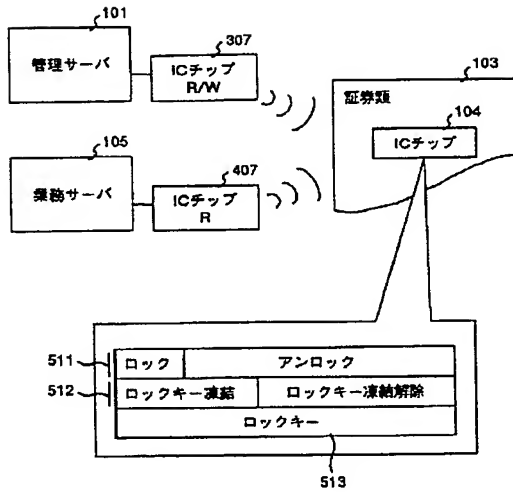
【図7B】実施形態の管理サーバ101のロック／ロックキー処理部310の処理手順を示すフローチャート（続き）である。

【符号の説明】

101…管理サーバ、103…証券類、104…ICチップ、105…業務サーバ、308…ロックキー管理テーブル、310…ロック／ロックキー処理部、511…ロック情報、512…ロックキー凍結情報、513…ロックキー

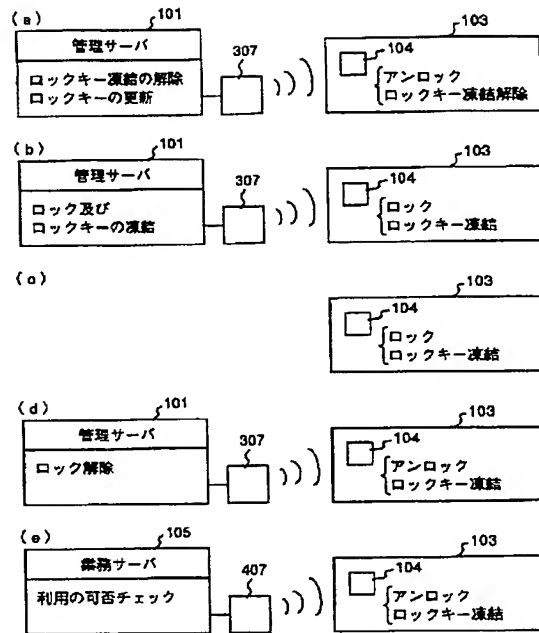
【図1】

図 1



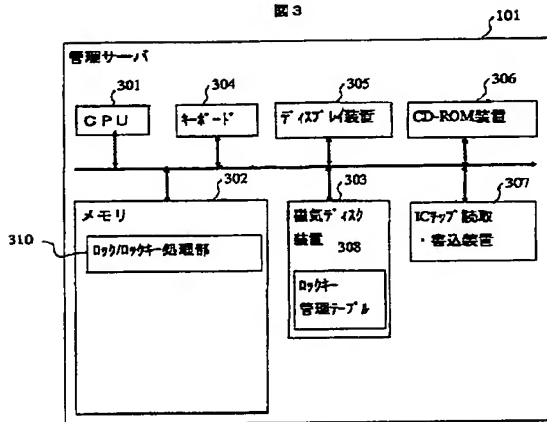
【図2】

図 2



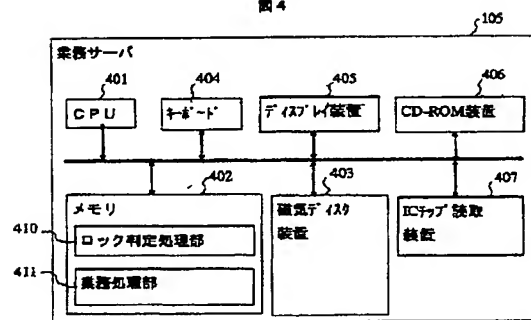
【図3】

図 3



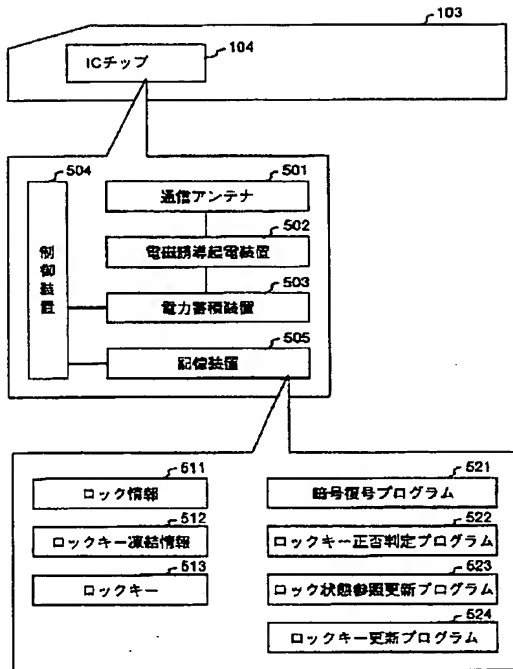
【図4】

図 4



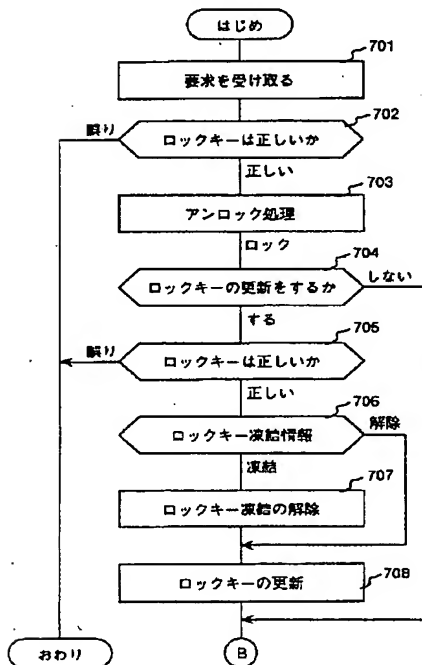
【図5】

図 5



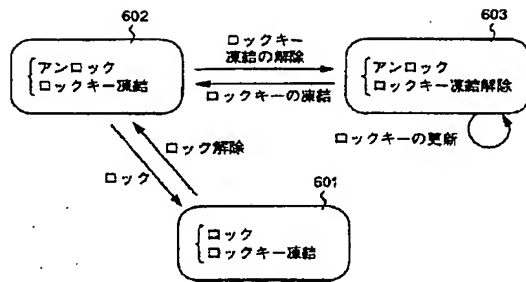
【図7A】

図 7 A



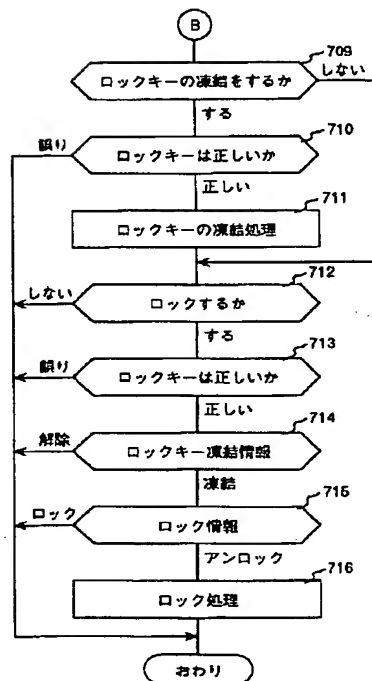
【図6】

図 6



【図7B】

図 7 B



(10)

特開2001-260580

フロントページの続き

(51)Int.Cl.⁷

識別記号

F 1

テーマコード(参考)

G 0 6 K 17/00

G 0 6 K 17/00

- L 5 B 0 5 8

19/07

G 0 7 D 7/02

F

19/00

G 0 6 K 19/00

H

G 0 7 D 7/02

Q

Fターム(参考) 2C005 HA01 HA02 HB10 JA09 JB40
LB20 LB32 MA01 MA03 MA40
MB10 NA09 PA02 QA05 SA06
SA07 SA08
3E041 AA01 AA02 AA03 BA20 BB07
DB01
5B035 AA13 BA01 BB09 CA23
5B049 AA05 BB47 CC39 DD01 DD04
DD05 EE03 EE23 EE25 EE28
FF03 FF04 FF08 FF09 GG03
GG06 GG10
5B055 CC10 CC13 EE02 EE13 EE17
EE21 EE27 HA12 JJ05 KK05
KK09 KK18 PA02 PA34
5B058 CA15 KA01 KA31 KA35